Wachtell, Lipton, Rosen & Katz

Risk Management and the Board of Directors

Martin Lipton
Daniel A. Neff
Andrew R. Brownstein
Steven A. Rosenblum
John F. Savarese
Adam O. Emmerich
David M. Silk
Wayne M. Carlin
William D. Savitt
David B. Anders
Andrea K. Wahlquist
Karessa L. Cain
Sarah K. Eddy
Sabastian V. Niles
Ryan A. McLeod
Anitha Reddy
Carol Miller
Carmen X. W. Lu
Jeohn Salone Favors
Raeesa I. Munshi
Ram Sachs

August 2021

Risk Management and the Board of Directors

I. INTRODUCTION

Overview

Over the past eighteen months, the Covid-19 pandemic provided a dramatic and unexpected pressure test of companies' risk management systems and practices. The pandemic has accelerated technological disruption and business model changes and exposed sharp differences in the impacts felt by different sectors, with some experiencing enormous dislocation and others doing remarkably well and arguably emerging stronger. More than two-thirds of organizations surveyed by the American Institute of Certified Public Accountants (AICPA) perceived an increased volume and complexity of risks in 2021—a higher number than even during the 2008-09 financial crisis. For example, the World Economic Forum's Global Risks Report 2021 emphasized new corporate risks arising from societal tensions, geopolitical fragmentation, environmental degradation and the potential for a "disorderly shakeout, threatening to create a large cohort of workers and companies that are left behind in the markets of the future." Now that vaccinations have proven effective in mitigating the risks of Covid-19, paving the way for an eventual sustained return of more favorable conditions, boards have the opportunity to reflect on how risk management policies weathered the Covid storm and to look forward to potential changes and enhancements that might be adopted in light of lessons learned. More broadly, corporate management and directors are coming under increasing pressure to manage in the interest of all stakeholders, increasing the importance of enterprise-level risk management, while courts and regulators are increasingly scrutinizing the presence and effectiveness of board-level risk oversight systems, adequacy of public disclosures and the quality of board response when crises erupt.

After all, managing corporate risk is not simply a business and operational responsibility of a company's management team—it is a governance issue that is squarely within the oversight responsibility of the board. Directors face a risk governance landscape that continues to evolve. This guide highlights a number of issues that have remained critical over the years or gained new salience during the pandemic. It also provides updates on Delaware law governing director liability—including developments that highlight the importance of active, engaged board oversight of corporate risk and maintaining appropriate records of that oversight. Key topics addressed in this guide are:

- the distinction between risk oversight and risk management;
- the tone at the top and corporate culture as components of effective risk management;
- recent developments in Delaware law regarding fiduciary duties and other legal frameworks;
- third-party guidance on risk oversight best practices;

- the strong institutional investor focus on risk matters;
- specific recommendations for improving risk oversight;
- U.S. Department of Justice guidance on the design of compliance programs;
- special considerations pertaining to ESG and sustainability-related risks;
- special considerations regarding cybersecurity, ransomware and data privacy matters; and
- anticipating future risks and the road ahead.

Risk Oversight by the Board—Not Risk Management

Both the law and practicality continue to support the proposition that the board cannot and should not be involved in day-to-day risk *management*. However, as recent legal developments make clear, it is important that the board's *oversight* includes active engagement in monitoring key corporate risk factors, including through appropriate use of board committees. These board-level monitoring efforts should be documented through minutes and other corporate records.

Directors should—through their risk oversight role—require that the CEO and senior executives prioritize risk management. Directors should satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite; that these policies and procedures are functioning as directed; and that necessary steps are taken to foster an enterprise-wide culture that supports appropriate risk awareness, behavior and judgments about risk and that recognizes and appropriately addresses risktaking that exceeds the company's determined risk appetite. The board should be familiar with the type and magnitude of the company's principal risks, especially concerning "mission critical" areas, and should be kept apprised periodically of the company's approach to mitigating such risks, instances of material risk management failures and action plans for mitigation and response. In prioritizing such matters, the board can send a message to management and employees that comprehensive risk management is not an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program, but is, instead, an integral component of strategy, culture and business operations.

Tone at the Top and Corporate Culture as Key to Effective Risk Management

The Covid-19 pandemic has placed a significant strain on many companies and highlighted the critical importance of ensuring that the board and relevant committees work with management to set the appropriate "tone at the top" by promoting and actively cultivating a corporate culture and environment that meets the board's expectations and aligns with the company's strategy. In setting the appropriate tone at the top, transparency, consistency and communication are key.

The board's vision for the corporation should include its commitment to risk oversight, ethics and avoiding compliance failures, and this commitment should be communicated effectively throughout the organization. Particularly where employee safety is concerned and at companies and in industries where product or service failures can jeopardize consumer or environmental safety, critical infrastructure or human life, the corporate culture should not, deliberately or due to inattention or insufficient resource allocation, prioritize cost-cutting or profits (which may include, as a matter of employee and public perception, compensation levels) over safety and compliance. In a 2021 AICPA report, 41% of organizations cited competing priorities as a barrier to effective enterprise risk management.

Continued developments regarding sexual and other misconduct in the workplace, as well as initiatives to promote diversity, inclusion and equity, also underscore the importance of setting the appropriate tone at the top. Harassment can have a devastating impact, first and foremost, on the employees targeted by such behavior. It can also have a significant impact on broader corporate culture, employee morale and retention, consumer preferences and the reputation of the company as a whole and the members of the board and the executive management team as individuals. Delayed or indecisive responses to sexual misconduct or discrimination can often be as damaging to a company as the misconduct itself. Similarly, ensuring an inclusive workplace environment is an important component of corporate culture—one that is central to employee morale and a motivated workforce.

With respect to these and other critical risks, the board should work with management to consider developing a crisis response plan that includes the participation of human resources officers, public relations advisors and legal counsel. The use, scope and design of preventative corporate policies, including training and educational programming, related to conduct and reporting expectations should also be carefully considered, as should potential implications, enforcement, remedies and application in the event of a violation once such policies are adopted. Disclosure of board-level participation in these deliberations also may be key to demonstrating to internal and external audiences the seriousness of these policies.

Promoting Board Readiness for Current and Future Risk Oversight

The evolution of risks has quickened in recent years, requiring boards to take a more active approach in ensuring directors have the skills to effectively oversee a company's pressing and emerging risks. The NACD's Blue Ribbon Commission report, "Fit for the Future," notes that director recruitment continues to prioritize "classic skills and experiences," such as executive leadership and finance, while under 5% of directors have experiences in emerging focus areas such as human capital and cybersecurity. To prepare for such risks, boards will certainly need to engage in director training to build on existing skills. In addition, the recruitment of new directors will need to address any potential gaps. Such recruitment efforts may require the board to move away from approaches that seek to replicate the skillset and experiences of existing directors. Indeed, boards are increasingly looking toward diverse candidates at various points in their careers to strengthen risk oversight capabilities.

II. SOURCES OF RISK OVERSIGHT OBLIGATIONS OF THE BOARD OF DIRECTORS

Although institutional investors, legislators and other constituencies have their own, varying expectations concerning board risk oversight responsibilities, the core responsibilities are grounded principally in state law fiduciary duties, federal and state laws and regulations, stock exchange listing requirements and certain established (albeit evolving) best practices.

Fiduciary Duties

The Delaware courts have taken the lead in formulating legal standards for directors' risk oversight duties, particularly following *In re Caremark International Inc. Derivative Litigation*, the seminal 1996 decision addressing director liability for the corporation's failure to comply with external legal requirements. Delaware courts in the *Caremark* line of cases have held that directors can be liable for a failure of board oversight only where there is "sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists" or a culpable failure to monitor an existing system resulting in a disregard of a pattern of "red flags." Delaware Court of Chancery decisions in the decades following *Caremark* regularly dismissed shareholder suits claiming such a total failure of oversight responsibility. *See*, for example, our memos discussing *In re The Goldman Sachs Group, Inc. Shareholder Litigation* (2011), *Oklahoma Firefighters Pension & Retirement System* v. *Corbat* (2017) and *City of Birmingham Retirement and Relief System* v. *Good* (2017).

More recent rulings, however, show that the risk of exposure for failure of oversight is real, and that courts are willing to permit shareholder claims alleging breaches of fiduciary duty by directors to go forward where the complaint alleges with specificity that red flags reflecting underlying compliance, safety, reporting or other risks were ignored or that insufficient board-level attention was paid to such matters, despite the existence of company-wide policies and procedures on the topic. These decisions have accepted well-pled claims that boards failed to act in good faith to maintain board-level systems for monitoring mission-critical functions, such as product safety, pharmaceutical trial testing and financial reporting. Histories of unaddressed deficiencies or a failure by the company to come forward with books and records evidencing meaningful board-level oversight have been among the chief aggravating factors driving these judicial decisions. *See, e.g.*, *Hughes* v. *Hu*; *Marchand* v. *Barnhill* (Bluebell Creameries); *In Re Clovis Oncology Inc. Derivative Litigation*.

Whether such lawsuits risk ripening into fiduciary liability will often turn on whether the targeted company can persuade a court that it had in place control and monitoring functions commensurate with the scope and scale of the potential risk. Once a *Caremark* claim survives a pleadings motion, it becomes a vehicle for extensive discovery and takes on substantial settlement value, even if not meritorious.

Ultimately, the events preceding oversight litigation illustrate that risk cannot be contained entirely. Corporate trauma can happen, even to the best-run companies, and courts can be expected to permit multiple avenues of litigation attack when it does. The best approach is for boards to undertake regular review of "mission critical" corporate operations and developments

affecting enterprise-level risk. As important, directors should create a clear written record of their review and their vigilant response to any compliance risks that may emerge, such that inspecting stockholders and reviewing courts will have a fair picture of directors' work. Boards that take care to institute and document such regular reviews will be in accord with best practices for corporate risk management. In the litigation context, boards will have a powerful answer, available at the pleading stage, if ever charged with neglecting their oversight duties.

SEC Risk Disclosure Rules

The SEC requires companies to disclose the board's role in risk oversight, the relevance of the board's leadership structure to such matters and the extent to which risks arising from a company's compensation policies are reasonably likely to have a "material adverse effect" on the company. A company must further discuss how its compensation policies and practices, including those of its non-executive officers, relate to risk management and risktaking incentives. Upcoming SEC rulemakings may expand expectations concerning cybersecurity, climate change, human capital management and other ESG and sustainability-related matters.

On a more granular level, the SEC requires companies to disclose in their annual reports "factors that make an investment in [a registrant's securities] speculative or risky." This expansive directive was until a few years ago accompanied by risk factor examples set forth in Item 503(c) of Regulation S-K (now Item 105), but the SEC eliminated those specific examples out of concern that they were encouraging "boilerplate" disclosures of limited value to investors. In August 2020, in furtherance of its "principles-based approach" to risk factor disclosure, the SEC adopted rule amendments to Item 105, noting that the amendments are designed to "result in risk factor disclosure . . . more tailored to the particular facts and circumstances of each registrant" and reduce use of "generic risk factors." Thus, companies must now disclose, in a concise and logical fashion, the most significant risks and explain how each factor affects the company's business and securities.

Early in the pandemic, the SEC supplemented its risk disclosure guidance with statements addressing the particular challenges posed by Covid-19. It called on public companies to use their earnings calls not merely as a forum to showcase historical financial results, but rather as an opportunity to address more pressing issues of how the company was responding and adapting to Covid-19, and how its financial condition might change in light of the pandemic. A March 2020 statement of the SEC's Division of Corporation Finance reiterated this invitation, asking companies to "proactively revise and update disclosures as facts and circumstances change." Addressing the concern that prospective statements along these lines might tend to invite litigation, the SEC encouraged companies to take advantage of available safe harbors, and gave assurance that it "would not expect good faith attempts to provide appropriately framed forward-looking information to be second guessed by the SEC." Illustrating how companies can fall short of these objectives, in December 2020, the SEC brought its first enforcement action against a public company related to Covid-19 financial disclosures by filing a settled administrative proceeding against The Cheesecake Factory, in which the company neither admitted nor denied the SEC's findings. While the respondent in this case had publicly stated that its restaurants were "operating sustainably" during the Covid-19 pandemic, according to the SEC, internal documents showed that at the time the company was

actually losing millions per week, had limited cash on hand and had notified its landlords that it would not be paying rent due to the adverse impact of Covid-19 on its business.

Stock Exchange Rules

New York Stock Exchange (NYSE) corporate governance standards impose certain risk oversight obligations on the audit committee of a listed company. Specifically, while acknowledging that "it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk," the NYSE requires that an audit committee "discuss guidelines and policies to govern the process by which risk assessment and management is undertaken." These discussions should address major financial risk exposures and the steps management has taken to monitor and control such exposures, including a general review of the company's risk management programs. The NYSE permits a company to create a separate committee or subcommittee to be charged with the primary risk oversight function as long as the risk oversight processes conducted by that separate committee or subcommittee are reviewed in a general manner by the audit committee and the audit committee continues to discuss policies with respect to risk assessment and management.

Dodd-Frank

The Dodd-Frank Act, which was enacted in the wake of the 2008 financial crisis, created new federally mandated risk management procedures principally for financial institutions. Dodd-Frank requires bank holding companies with total assets of $10 billion or more, and certain other non-bank financial companies, to have a separate risk committee that includes at least one risk management expert with experience managing risks of large companies.

Third-Party Guidance on Best Practices

Various industry-specific regulators and private organizations publish suggested best practices for board oversight of risk management. Examples include reports by the National Association of Corporate Directors (NACD) Blue Ribbon Commission on Risk Governance, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Conference Board.

In 2017, COSO released its updated internationally recognized enterprise risk management framework, which originated in 2004. The updated framework consists of five interrelated components of enterprise risk management: (1) Governance and Culture (the tone of the organization, which reinforces the importance of enterprise risk management and establishes oversight responsibilities for it); (2) Strategy and Objective-Setting (the integration of enterprise risk management into the organization's strategic plan through the process of setting strategy and business objectives); (3) Performance (the identification and assessment of risks that may impact achievement of strategy and business objectives); (4) Review and Revision (the review of the organization's performance, which allows for consideration of how well the enterprise risk management components are functioning and what revisions are needed); and (5) Information, Communication and Reporting (the continual, iterative process of obtaining information, from both internal and external sources, and sharing it throughout the organization).

Recognizing that calls for identifying and mitigating ESG risks have become increasingly urgent, COSO, in conjunction with the World Business Council for Sustainable Development, released guidance in 2018 for applying enterprise risk management to ESG-related risks. This guidance recognizes that companies "face an evolving landscape of environmental, social and governance (ESG)-related risks that can impact their profitability, success and even survival" and that such risks have "unique impacts and dependencies." Notably, the guidance reaches social-related risks encompassing stakeholder opposition, supply chain matters, human capital and labor-related issues and the complex area of maintaining "'social license' to operate." The guidance offers an enterprise risk management approach that runs from governance to risk identification and assessment through to communication and reporting.

COSO released additional guidance in November 2020 regarding the nexus between enterprise risk management and compliance risk management. The guidance aims to address management of risks related to adhering to specific laws and regulations, as well as adjacent risks related to compliance with professional standards, internal organizational policies and contractual obligations. Importantly, it acknowledges that compliance risks may arise not only from insider action—of directors, management and employees—but also third parties such as suppliers, outside sales representatives and contractors.

In July 2020, the Institute of Internal Auditors (IIA) released an update to its twenty-year-old "Three Lines of Defense" model in risk management, now named the "Three Lines Model." The updated name reflects a reorientation from defending against risk toward value creation and prospective risk management. More substantively, the model reconfigures the parties involved in risk management. Under the prior version of the model, (1) management control was the first line of defense, (2) various risk control and compliance oversight functions established by management were the second line of defense, and (3) independent assurance was the third line of defense. The updated model incorporates the governing body and makes it accountable to stakeholders for organizational oversight. In addition, the model's departure from the strict "three lines" approach highlights the need for collaboration and communication between the governing body, management and internal audit functions.

Both COSO and IIA, as well as other frameworks outlining risk-related best practices, underscore that risk oversight and risk management should not be treated as isolated, defensive functions, but rather should be proactively integrated into strategic planning and prioritized as part of board- and CEO-level governance and oversight.

III. STRONG INVESTOR FOCUS ON RISK MANAGEMENT CONTINUES

Institutional Investors

Risk oversight is a top governance priority of institutional investors. In recent years, investors have pushed for more meaningful and transparent disclosures on board-level activities and performance with respect to risk oversight. As noted in the NACD's Blue Ribbon Commission report on disruptive risks, investors "keep raising the bar for boards on the oversight of everything from cybersecurity to culture, and the notion of companies' license to operate is now front and center." As further discussed below, this investor focus has become especially acute in the area of ESG and sustainability-related risks.

Major institutional investors such as BlackRock, State Street and Vanguard believe that sound risk oversight practices are key to enhancing long-term, sustainable value creation. BlackRock has said that it expects boards to have "demonstrable fluency" in areas of key risks affecting the company's business and in management's approach to addressing and mitigating those risks, and that it will assess this through corporate disclosures and, if necessary, direct engagement with independent directors. BlackRock is particularly interested in understanding the evolution of risk oversight processes in response to changes in strategy or the business risk environment. It has also said it will not hesitate to vote against certain directors that it deems responsible for risk oversight weaknesses. Indeed, in "aim[ing] to be the voice of the long-term investor," BlackRock's stewardship approach involves "urging companies to focus on the governance and sustainability risks that can impact their ability to generate long-term financial returns," driven by a belief that "company valuations can be significantly influenced by these risks." State Street has likewise emphasized that "good corporate governance necessitates the existence of effective internal controls and risk management systems, which should be governed by the board," and that it will actively seek direct dialogue with the board and management of companies to "protect longer-term shareholder value from excessive risk due to poor governance and sustainability practices." Vanguard, for its part, has said that it views directors as "shareholders' eyes and ears on risk" and relies "on a strong board to oversee the strategy for realizing opportunities and mitigating risks." Vanguard reiterated this sentiment in its 2021 Investment Stewardship Annual Report, noting, "When we discuss strategy and risk with portfolio companies, we work to assess how well the board of directors understands the company's strategy and how deeply it is involved in identifying and governing material risks." Like other institutional investors, Vanguard cited the pandemic as an example of "unpredictable crises" where "strong oversight practices enable a board to steer a company."

Proxy Advisory Firms

In exceptional circumstances, scrutiny from institutional investors with respect to risk oversight can translate into shareholder campaigns and adverse voting recommendations from proxy advisory firms such as Institutional Shareholder Services (ISS) and Glass Lewis. Both ISS and Glass Lewis will recommend voting "against" or "withhold" in director elections, even in uncontested elections, when the company has experienced certain extraordinary circumstances, including material failures of risk oversight.

In the 2021 update to its Global Proxy Voting Guidelines, ISS clarified that a significant oversight failure relating to an environmental or social concern may constitute a material governance failure triggering a vote recommendation against board members. Previously, ISS added risk oversight failures to the set of factors that will increase the likelihood of the proxy advisory firm supporting an independent chair proposal—specifically, "evidence that the board has failed to oversee and address material risks facing the company" or evidence of "a material governance failure." The ISS ESG Governance QualityScore—a data-driven scoring and screening tool that ISS is encouraging institutional investors to use to monitor portfolio company governance—also focuses heavily on boards' audit and risk oversight. ISS has noted that failures of risk oversight include, but are not limited to, bribery, large or serial fines or sanctions from regulatory bodies and significant adverse legal judgments or settlements. ISS has also called out risk oversight related to the Covid-19 pandemic as a particular area of focus and concern, warning that "[c]ompanies that fail to safeguard the health of their

employees, or whose business continuity plans prove to be inadequate, could eventually face" adverse action in the form of low shareholder support for reelection of certain directors.

Meanwhile, for the 2020 proxy season, Glass Lewis made noteworthy revisions to its proxy voting guidelines to reflect its approach to evaluating board oversight of ESG risks in particular. "[F]or large cap companies and in instances where [Glass Lewis] identif[ies] material oversight issues, Glass Lewis will review a company's overall governance practices and identify which directors or board-level committees have been charged with oversight of environmental and/or social issues" and "also note instances where such oversight has not been clearly defined" in the company's governance documents. Where Glass Lewis believes "that a company has not properly managed or mitigated environmental or social risks," or that "such mismanagement has threatened shareholder value, Glass Lewis may consider recommending that shareholders vote against" those directors "who are responsible for oversight of environmental and social risks. In the absence of explicit board oversight of environmental and social issues, Glass Lewis may recommend that shareholders vote against members of the audit committee." In its 2021 proxy voting guidelines, Glass Lewis added that it would highlight when boards do not "provide clear disclosure concerning the board-level oversight afforded to environmental and/or social issues" and, beginning in 2022, will recommend against the governance chair of such companies.

IV. RECOMMENDATIONS FOR IMPROVING RISK OVERSIGHT

The board should seek to promote an effective, ongoing risk dialogue with management, design the right relationships across the board, its committees, management, and the workforce regarding risk oversight, and ensure that appropriate resources support risk management systems, compliance, and reporting mechanisms. While risk management should be tailored to the specific company and relevant risks, in general, an effective risk management system will: (1) adequately identify the material risks that the company faces in a timely manner; (2) adequately transmit necessary information to senior executives and, importantly, to the board or relevant board committees; (3) implement appropriate risk management strategies that are responsive to the company's risk profile, business strategies, specific material risk exposures and risk tolerance thresholds; (4) integrate consideration of risk and risk management into strategy development and business decision-making throughout the company; (5) feature regular reviews of the effectiveness of the company's risk management efforts, on a quarterly or semiannual basis; and (6) document the existence of risk management protocols and appropriate board-level engagement on risk matters.

Specific Recommendations

Below are specific actions the board and appropriate board committees should consider as part of their risk management oversight:

- review with management the categories of risk the company faces, including any risk concentrations and risk interrelationships, as well as the likelihood of occurrence, the potential impact of those risks, mitigating measures and action plans to be employed if a given risk materializes;

- review with management the company's risk appetite and risk tolerance, its tools for measuring company-wide risks and assessing risk limits and whether the company's business strategy is consistent with the agreed-upon risk appetite and tolerance;

- review with management the primary elements comprising the company's risk culture, including establishing "a tone from the top" that reflects the company's core values and the expectation that employees act with integrity and promptly escalate noncompliance in and outside of the organization, and steps to ensure effective communication of the company's risk management strategy throughout the organization and through appropriate public disclosures;

- review the company's director, executive and employee compensation structure and incentive programs to ensure they are appropriate in light of the company's articulated risk appetite and that these programs are creating incentives to encourage, reward and reinforce desired corporate behavior;

- review with committees and management the board's expectations as to each group's respective responsibilities for risk oversight and management to ensure a shared understanding as to roles and accountability, including the quality, format and cadence of management's risk reporting to the board and/or appropriate committees;

- review with management the design and independence of the company's risk management functions, as well as the qualifications and backgrounds of senior risk officers and the resources available to and policies applicable to risk management personnel, to assess whether they are appropriate given the company's size and scope of operations, and to assure the prompt and coherent flow of risk-related information within and across business units; and

- review the skills, professional experiences and practices that are required by the board to effectively oversee risks, to assess whether the current board's mix of skills and professional experiences are sufficient and identify selection priorities to be used as part of the board recruitment and refreshment process.

The board should formally review, on at least an annual basis, the company's risk management system, including a review of board- and committee-level risk oversight policies and procedures and a presentation of "best practices" to the extent relevant, tailored to focus on the industry or regulatory arena in which the company operates. In the wake of the recent Delaware decisions green-lighting *Caremark* claims across a variety of industries, directors should also implement effective procedures to ensure that the board itself monitors key enterprise risk on an ongoing basis and properly documents this monitoring. To this end, it may be appropriate for boards and committees to engage outside consultants to assist them both in the review of the company's risk management systems and in understanding and analyzing business-specific risks. But because risk, by its very nature, is subject to constant and unexpected change, annual reviews cannot replace the need to regularly assess and reassess company operations and processes, learn from past mistakes and external events, and seek to ensure that current practices

enable the board to address specific major issues whenever they may arise. Where a major or new risk event comes into focus, management should investigate and report back to the full board or the relevant committees as appropriate.

While fundamental risks to the company's business strategy are often discussed at the full board level, many boards continue to delegate primary oversight of risk management to the audit committee, which is consistent with the NYSE corporate governance standard requiring the audit committee to discuss risk assessment and risk management policies. In recent years, the percentage of boards with a separate risk committee has grown, but that percentage remains relatively low. According to a 2020 Spencer Stuart survey, only 13% of the companies surveyed had a standing risk committee. As discussed earlier in this memo, companies subject to Dodd-Frank are required to have a dedicated risk management committee. However, the appropriateness of a dedicated risk committee at other companies will depend on the industry and specific circumstances of the company. If the company keeps the primary risk oversight function within the audit committee, the audit committee should schedule periodic review of risk management outside the context of its role in reviewing financial statements and accounting compliance. The potential for overload is real: a KPMG survey found that 39% of audit committee members find it difficult to oversee major risks in addition to carrying out core oversight responsibilities.

Thoughtfully allocating responsibility for risk management and compliance among the board's committees also creates an opportunity for alignment of officer-to-board-level reporting relationships, which has the added value of ensuring that the directors get to know and regularly communicate with a broader range of corporate executives. In an era in which the number of insiders on a company's board is usually just one or two—generally the CEO and perhaps one additional director—board/management alignment gives the board direct insight into the company's operations and culture.

Any committee charged with risk oversight should hold sessions in which it meets directly with key executives primarily responsible for risk management. It may also be appropriate for the committee(s) charged with risk oversight to meet in executive session both alone and together with other independent directors to discuss the company's risk culture, the board's risk oversight function and key risks faced by the company. In addition, senior risk managers and senior executives should understand they are empowered to inform the board or committee of extraordinary risk issues and developments that require immediate board attention outside the regular reporting procedures. In light of the *Caremark* standards discussed above, the board should feel comfortable that it receives reports of red flags or "yellow flags," so that such issues may be investigated as appropriate.

Department of Justice Guidance on the Design of Effective Compliance Programs

Senior management should provide the board or committee with an appropriate review of the company's legal compliance programs and how they are designed to address the company's risk profile and detect and prevent wrongdoing. While compliance programs will need to be tailored to the specific company's needs, the board and senior management of any

company should establish a strong tone at the top that emphasizes the company's commitment to full compliance with legal and regulatory requirements, as well as internal policies.

This goal is particularly important not only to reduce the risk of misconduct, but also because a well-tailored compliance program and a culture that values ethical conduct are critical factors that the DOJ will assess in considering whether to bring charges against a corporation in the event that corporate personnel engage in misconduct. Under the Principles of Federal Prosecution, prosecutors are required to weigh the seriousness of the offense, the role (if any) of high-level management, the effectiveness of a company's compliance program at the time of the offense, the extent of cooperation and reporting, remedial measures taken and potential collateral consequences for innocent stakeholders. In addition, under the DOJ's FCPA Corporate Enforcement Policy, which serves as non-binding guidance in all Criminal Division corporate fraud investigations, a company is only eligible for the full range of benefits—including a declination—if it has implemented an effective ethics and compliance program. Finally, under the DOJ's recently updated guidance for white-collar prosecutors, which identifies factors to be considered in evaluating corporate compliance programs, prosecutors may "reward efforts to promote improvement and sustainability" of compliance programs in the form of any prosecution or resolution. Thus, companies with robust compliance programs that continually improve based on lessons learned and data gathered have a real opportunity to benefit.

Directors should consider borrowing from the updated DOJ guidance by constructively posing many of the same probing questions that the DOJ now expects federal prosecutors to ask. Those DOJ directives are aimed at understanding the same fundamental questions a well-informed director should want to understand: Is the company's compliance program well-designed, adequately resourced, drawing upon the right information and data and effective at driving the right ethics and compliance messages throughout the organization? Management should be expected to provide the board or appropriate board committees with timely and complete answers to these kinds of questions, and do so periodically.

In keeping with the DOJ's guidance, a compliance program should be designed by people with relevant expertise and will typically include interactive training as well as written materials. Compliance policies should be reviewed periodically to assess their effectiveness, to ensure they target the company's current compliance risks and to make any necessary changes. Policies and procedures should fit with business realities. A rulebook that looks good on paper but which is not followed will end up hurting rather than helping. There should be consistency in enforcing stated policies through appropriate disciplinary measures. Finally, there should be clear reporting systems in place both at the employee level and at the management level so employees understand when and to whom they should report suspected violations and so management understands the board's or committee's informational needs for its oversight purposes. A company may choose to appoint a chief compliance officer and/or constitute a compliance committee to administer the compliance program, including by facilitating employee education and issuing periodic reminders. If there is a specific area of compliance that is critical to the company's business, the company may consider developing a separate compliance apparatus devoted to that area.

V. SPECIAL CONSIDERATIONS REGARDING ESG AND SUSTAINABILITY-RELATED RISKS

ESG risks represent a specific subset of general risks that a company should manage, by identifying and mitigating company-specific risks like environmental liabilities, labor standards, consumer and product safety and leadership succession, as well as contingency planning for macro-level risks. Supply chain and energy alternatives should be identified and backup recovery plans developed for climate change and other natural disaster scenarios. Broader sustainability-related risks, including the sustainability of a company's business model in the face of accelerating change, also merit focus and oversight. These issues are getting increased focus under the Biden administration. On March 4, 2021, the SEC announced the creation of the Climate and ESG Task Force in the Division of Enforcement, to focus on identifying misstatements in companies' disclosure of climate risks and gaps in existing disclosure requirements. The task force also will analyze disclosure and compliance issues relating to investment advisers' and funds' ESG strategies. In May 2021, the SEC's Acting Director of the Division of Corporation Finance indicated that new disclosure requirements would focus on three areas: diversity, equity and inclusion; climate change; and human capital management. In August 2021, SEC Chair Gary Gensler made clear that the SEC is actively considering near-term rulemaking that would encompass mandated climate change-related disclosures, including as to oversight and management of climate-related risks and opportunities and related qualitative and quantitative disclosures.

While boards have been overseeing management of ESG-related material risks for as long as they have existed, the social and economic turmoil caused by the global spread of Covid-19 has accelerated the focus on a number of traditional ESG concerns, including human capital issues, business model and supply chain resilience and consumer welfare and social impact, as well as matters of environmental stewardship. ESG factors will be critical elements of both short-term strategic decisions and longer-term strategic planning, and major institutional investors are increasingly engaging companies on whether ESG metrics are incorporated into executive and employee incentive opportunities in order to encourage achievement of the ESG-related goals included in such strategies. Boards should therefore ensure that ESG-related risks are being evaluated, disclosed and managed appropriately—and that a proper oversight structure at the board level, supported by appropriate management-level structures, is in place.

Investor Focus on ESG Risks

Major institutional investors increasingly view ESG issues as significantly affecting a company's long-term financial value. BlackRock has been one of the biggest proponents of this view, remarking that just as it expects companies to understand the macroeconomic and industry trends in which they operate, it also believes that a company's awareness of ESG-related trends helps drive long-term performance and mitigate risk. In his 2021 letter to CEOs, BlackRock's Chairman and CEO, Laurence D. Fink, noted the impact of the pandemic on reaffirming a focus on ESG, and in particular, climate change: "I believe that the pandemic has presented such an existential crisis—such a stark reminder of our fragility—that it has driven us to confront the global threat of climate change more forcefully and to consider how, like the pandemic, it will alter our lives." Fink has previously made clear that BlackRock endorses the industry-specific guidelines developed by the Sustainability Accounting

Standards Board as well as the climate-specific recommendations developed by the Task Force on Climate-related Financial Disclosures as benchmark frameworks for ESG disclosure. Fink has stressed that "we [BlackRock] strongly support moving to a single global standard, which will enable investors to make more informed decisions about how to achieve durable long-term returns. Because better sustainability disclosures are in companies' as well as investors' own interests, I urge companies to move quickly to issue them rather than waiting for regulators to impose them." BlackRock also includes consideration of ESG risk oversight and disclosures in assessing whether to vote or consider voting against committee members and/or individual directors in its proxy voting guidelines.

State Street has taken a similar approach to ESG. On January 11, 2021, State Street's CEO Cyrus Taraporevala released his annual letter on SSGA's 2021 proxy voting agenda in which he announced that its main stewardship priorities for 2021 will be the systemic risks associated with climate change and a lack of racial and ethnic diversity at both the board and workforce levels.

Recommendations for Improving ESG Risk Oversight

In large part, a board's function in overseeing management of ESG-related risks involves issue-specific application of the risk oversight practices discussed in this guide. The board should work with management to identify ESG issues that are pertinent to the business and its stakeholders and decide what policies and processes are appropriate for assessing, monitoring and managing ESG risks, as well as how to incentivize proper management of these risks. The board should also be comfortable with the company's approach to external reporting and shareholder engagement regarding the company's overall approach, response and progress on ESG issues. And it is increasingly important for directors and management who engage with shareholders to educate themselves and become conversant on the key ESG issues facing the company. Companies are also wise to assess whether there are ESG-related opportunities to be factored into business strategy.

As a practical matter, boards can familiarize themselves with all of these ESG-related matters through periodic management briefings. Creating a more focused board committee or subcommittee, such as a "corporate responsibility and sustainability" committee, that is specifically tasked with oversight of specified ESG matters, or updating existing committee charters and board-level corporate governance guidelines to address the board's approach to such topics, may also be considered, although there is no one-size-fits-all approach to board oversight of ESG risks. Of course, the board should ensure that any committee tasked with ESG risk oversight properly coordinates with any other committees tasked with other types of risk oversight (*e.g.*, the audit committee) and that the board as a whole is satisfied as to the company's approach on these matters and sufficient flexibility is retained within at the board level to respond to new ESG issues.

VI. SPECIAL CONSIDERATIONS REGARDING CYBERSECURITY, RANSOMWARE, AND DATA PRIVACY RISKS

Cybersecurity increasingly has become a risk factor that requires special attention—both because it affects all aspects of most businesses and because failure to

adequately identify, control and mitigate cyber risk can be devastating. The events of the past 18 months, which led the Biden administration to issue multiple Executive Orders declaring cyber threats a "top priority and essential to national and economic security," have only underscored this need. The risk of targeted attacks from criminal groups, foreign intelligence services and other bad actors has increased with the mass shift to remote work arrangements, embrace of cloud-based operations and increased reliance on virtual commerce spurred by the pandemic. Among risk management leaders, 65% see increased risk related to cybersecurity and data protection, according to the 2021 PwC Pulse Survey. We have seen this risk manifested in the ransomware attack that shut down one of the country's largest pipelines for refined petroleum products, and in the massive SolarWinds attack. These incidents, among many others, underscore the imperative that companies diligently consider cybersecurity risks, mitigate vulnerabilities, engage in active defense, leverage law enforcement resources and third-party specialists identified in advance and plan for a robust and rapid incident response.

At the same time, legal and regulatory demands on companies to safeguard consumer data, protect against intrusions, and make related disclosures to government agencies, stockholders and the public have stepped up significantly in recent years. The EU's General Data Protection Regulation (GDPR), which took effect in 2018, has transformed data handling obligations of companies whose operations have even a minimal European nexus, as has domestic legislation like the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, the California Privacy Rights Act of 2020, which amends and expands the CCPA, and the new Virginia Consumer Data Protection Act, which was signed into law in March 2021.

Federal and state agencies have made cybersecurity a focus, bringing attention-grabbing enforcement actions for failure to abide by their overlapping webs of requirements. In November 2020, a little over a year after its historic data privacy settlement with Facebook, the Federal Trade Commission (FTC) announced a settlement with Zoom for alleged misrepresentations to consumers about encryption levels and how some versions of its software circumvented web browser safeguards intended to protect users from risk of remote video surveillance. This settlement is just one illustration of the FTC's increased enforcement activity in the data privacy and protection arena—a trend that we predict will persist unabated notwithstanding the recent Supreme Court decision cutting back the agency's ability to pursue disgorgement and restitution remedies. Another agency that has been particularly active of late is the New York State Department of Financial Services (NYDFS), which over the last year brought its first actions enforcing the detailed and prescriptive cybersecurity regulations it put in place in 2019.

There is a silver lining to the twin pressures of increased cyber risk and accompanying regulatory focus: more sophisticated and nuanced guidance to companies about what they should be doing to manage and disclose risk, and what boards of directors should be doing to oversee that risk management and disclosure. For example, the U.S. Department of the Treasury, Office of Foreign Assets Control and Financial Crime Enforcement Network in October 2020 issued advisories to assist in combating ransomware attacks and to comply with sanctions and anti-money laundering regulations. In February 2021, NYDFS issued two guidance memos, one addressing cyber insurance, and another recommending steps that entities with public-facing websites should take to prevent fraudulent access of nonpublic information.

The SEC, for its part, has had cybersecurity disclosure guidance in place since 2011, when the Division of Corporation Finance issued interpretive guidance requiring companies to "disclose the risk of cyber incidents if they are among the most significant factors that make an investment in the company speculative or risky." That guidance was clarified in 2018, and was supplemented in early 2020 by the Office of Compliance Inspections and Examinations' Cybersecurity and Resiliency Observations.

Given the recent uptick in ransomware attacks against companies across various industries, the White House, in June 2021, issued an unprecedented open letter to the private sector encouraging corporate leaders to view the specter of a ransomware attack as not just a potential vector for data compromise but also a direct threat to core business operations. The letter recommended that executives immediately convene their leadership teams to ensure that cyber defenses, as well as incident response, continuity and recovery plans were tailored to the evolving risk landscape. Later the same month, NYDFS issued guidance describing a number of ransomware prevention measures that NYDFS-regulated entities should integrate into existing cybersecurity programs.

Broadly speaking, the available regulatory and other guidance tracks the framework established by the National Institute of Standards and Technology (NIST), a critical benchmark that has been used and endorsed by the SEC and the FTC. The NIST elements are: identification of risk, protection of key data and systems, incident detection, incident response (including disclosure) and recovery. At the board level, the guidance is appropriately less operational and instead focused on ensuring that management is thinking about and addressing cyber risk in line with the company's risk profile and organizational goals and strategy. These principles are reflected, for example, in the April 2021 Board Cybersecurity Oversight Guidance issued by the World Economic Forum (WEF), the National Association of Corporate Directors and the Internet Security Alliance, in partnership with PwC, and in the WEF's May 2021 white paper entitled Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers.

In general, the applicable guidance and our experience teach that boards of directors should have the following in mind when it comes to cyber risk:

- Oversight Mechanism: Boards should carefully consider with management the avenues through which they monitor cyber risk. Although it is common to have the cyber risk oversight function fall to the audit committee, this should be carefully considered given the burden on audit committees. An alternative to consider, depending on the magnitude of the oversight responsibility, is the formation of a dedicated, cyber-specific board-level committee or sub-committee. At the same time, because cybersecurity considerations increasingly affect all operational decisions, they should be a recurring agenda item for full board meetings. Companies that already have standalone risk or technology committees should also consider where and how to situate cybersecurity oversight. The appointment of directors with experience in technology should be evaluated alongside board tutorials and ongoing director education on these matters.

- Review of Policies, Procedures & Resources: In carrying out their oversight function, directors should ensure that the company has written policies and procedures in place governing each of the NIST elements, and that both the cybersecurity and the internal audit functions include personnel with the necessary technical expertise and sufficient time and resources to devote to cybersecurity risk and review. A review of the common elements of remedial and other cyber-related enforcement actions brought by state and federal actors suggests a growing expectation among regulators that companies maintain written information security programs that senior management present to the board on at least an annual basis.

- Verification of Risk Identification & Assessment: Directors should have some understanding of the systems the company uses, and the data it collects, as well as the risks the company faces by virtue of how it uses technology and data collection and storage. While managing the cybersecurity-related risks of remote work arrangements is a task that virtually every company has taken on as a result of the pandemic, each company's cyber risk profile is unique. The role of directors is to ensure that a cyber risk assessment and mitigation system is in place at the company, that those managing the company's cybersecurity identify and consider potential vulnerabilities (leveraging the latest threat intelligence and best practices) and that the board is engaged in active oversight of such matters.

- Oversight of Protection & Detection Strategies: Directors should be briefed on management's plan for implementing appropriate protections against cyber intrusions and related risks, including programmatic efforts to detect and mitigate vulnerabilities and enable business continuity. In addition, directors and executives should maintain a sustained focus on the timely remediation of material cyber risks, whether identified by internal or external sources, and, where exposures or shortfalls are identified, confirm that appropriate protective or remedial recommendations are enacted without undue delay. Responsible personnel should be engaged in continuous monitoring and improvement efforts, including as to seemingly mundane but mission-critical tasks like timely patching of critical systems. Knowledgeable employees from the internal audit function should usually be involved as well.

- Oversight of Response Strategy and Disclosure Protocols: Directors should receive briefings from time to time on the procedures put in place by management to facilitate a swift, robust and effective response to a breach or other cybersecurity incident, as well as on the company's response to material cybersecurity incidents and related impacts. A company's response plan should cover all categories of likely incident scenarios, as well as unlikely but plausible scenarios with extreme consequences. The plan should address notification and response protocols, procedures for escalation to appropriate management personnel and ultimately the board, business and service interruption scenarios (including whether systems could or should be taken offline as a precautionary measure following a suspected breach) and communications with regulators and stakeholders. The company should also have a coherent and legally vetted plan for making appropriate and compliant disclosures and notifications to law enforcement, industry-specific regulators, consumers, and the public if and when data or other systems are materially compromised.

- Documentation of Board-Level Oversight: Finally, board and committee oversight activities, including in the aftermath of a material cyber incident that causes significant harm or disruption, should be appropriately documented in minutes and in supporting materials. Stockholder inspection demands to review a company's books and records, including board- and committee-level minutes, in preparation for litigation are increasingly common and allowed by the courts where certain pleading requirements are met.

VII. CONCLUSION

Anticipating Future Risks

Understanding risks inherent in the company's strategic plans, risks arising from the competitive landscape and potential for technology and other developments to impact the company's profitability and prospects for sustainable, long-term value creation is a critical element of any effective system for board-level oversight of risk. Gaining that understanding, of course, will allow boards and management to anticipate future risks, which, in turn, is critical to avoiding or mitigating those risks before they escalate into crises.

As stressed in the NACD's report, "Fit for the Future," boards are entering a time of both extreme challenge and promise:

> *The accelerating pace and intensifying complexity of change are leading to the emergence of a fundamentally different operating reality than incumbent executives and directors have experienced in their careers to date. However, this dizzying amount of change also creates immense opportunities for companies to out-innovate the competition, to generate value in new ways, and to strengthen their governance.*

The Road Ahead

Directors face an evolving risk and governance landscape, and boards are now recognized as having an affirmative obligation to use their business judgment in identifying material business and liability risks and working with management in articulating the strategy and the time horizon for mitigating them. The law is clear that properly informed directors are empowered to act to protect the corporate reputation and engender trust in the corporation; to understand and have the company take steps to mitigate mission-critical and other material risks; to pursue disclosure and engagement efforts designed to inform investors about global social and environmental developments that threaten long-term corporate health; to safeguard long-term global supply chain relationships; and to strengthen the ability to recruit, incentivize and retain a skilled and motivated workforce. Taken together, directors' duties not only permit boards to address the full range of risks that threaten the corporation's ability to deliver sustainable growth, but indeed require boards to address the most acute among them.

INDEX